Дюгуров Д.В.

СЕТИ С ОТКРЫТОЙ ИНФРАСТРУКТУРОЙ: БЕЗОПАСНЫЙ ИНСТРУМЕНТ ОБУЧЕНИЯ И ПРОИЗВОДСТВА

dvoe_sm@mail.ru
ГОУ ВПО "Удмуртский государственный университет"
г. Ижевск

Рассматривается ряд проблем, возникающих при организации общих сетевых ресурсов. В качестве решения предложен проект вычислительной сети с открытой инфраструктурой. Рассмотрены предметная область, необходимость и перспективы проекта, дано его техническое описание.

The problems arising at the organization of the common network resources is considered in article. The project of the computer network with an open infrastructure is offered as the decision of the problem. The subject domain, necessity and prospects of the project are considered, its description is given.

1. Введение

Создание и рациональное использование общих вычислительных ресурсов является одной из важнейших задач информатизации в целом. Возможность масштабирования сетей, интеграции между собой уже созданных сегментов напрямую зависит от выбранных сетевых платформ. Особую актуальность эта проблема приобретает в профильных ВУЗах. В данном случае учебному заведению необходимо решать сразу несколько задач:

- подготовка специалистов (программистов, системотехников, специалистов по безопасности информации и пр.), часто в отрыве от реальных производственных задач;
- необходимость привлечения денежных средств;
- соответствие технической базы требованиям времени;
- обеспечение функционирования и развития отрасли в регионе;

Для этого учебное заведение должно обладать высококлассными специалистами из числа профессорско-преподавательского состава, «рабочей силой» - студентами, и средством разработки. Таковым инструментом должна быть распределенная сеть, состоящая из мощных вычислительных машин, адекватных им операционных систем и сред разработки. Использование такого комплекса позволит учебному заведению получать заказы и выполнять реальные проекты. Тем самым погружать студентов в производственную среду не только без ущерба для учебного процесса, но и с огромной практической пользой.

В качестве решения всех названных выше задач предлагается проект вычислительной сеть на базе имеющихся в распоряжении факультета Информационных технологий и вычислительной техники УдГУ компьютеров, серверных операционных систем Microsoft Windows Server 2003 SP2, клиентских опе-

рационных систем Windows XP Professional SP 2 и лицензионных средств разработки, распространяемых для высших учебных заведений.

Масштабы данной сети будут сопоставимы с сетью крупного промышленного предприятия. Гарантированное использование студентами лицензионного программного обеспечения, установленного на факультетских серверах, позволит повысить культуру будущих специалистов и сократить количество ошибок в их продуктах.

Наличие данного инструмента должно породить особое содружество студентов: инициативные студенты, получая определенные заказы, могут формировать собственные команды, используя факультетскую сеть в качестве средства разработки. В дальнейшем, образовывая собственные компании, они могут продолжать использовать университетскую сеть и ее ресурсы. В результате вокруг университета сложится бизнес-окружение, которое будет потреблять выпускников соответствующих специальностей и снабжать студентов практической работой, что является идеальным вариантом для структуры высшего образования в целом. Также это позволит университету участвовать в выгодных коммерческих проектах и повысит престиж преподавательской деятельности среди бывших студентов, что обеспечит воспроизводство кадров для университета.

Описанную выше сеть далее назовем *вычислительной сетью с открытой инфраструктурой*. Причем «открытость» понимается в том смысле, что студентам, обучающимся в университете, известно о том, как организована часть данной сети, какие используются программные продукты и аппаратные средства. Также надо понимать, что такая «открытость» не является угрозой безопасности сети в целом.

Использование вычислительных сетей, организованных по такому принципу, может стать стандартом во всех государственных учреждениях. Это позволит интегрировать их в одну глобальную сеть с минимальным количеством трудозатрат.

2. Сеть с открытой инфраструктурой.

Технически инфраструктуру ЛВС можно рассматривать с двух позиций. *Первая* (2.1.) – с точки зрения структуры объединения компьютеров в группы и связей групп между собой. *Вторая* (2.2.) – с точки зрения объединения внутренней сети и внешнего Интернета. В дальнейшем мы рассмотрим ЛВС с обеих точек зрения по порядку.

Предположим, что корневым будет являться домен третьего уровня **fitvt.udsu.ru**. Поддомены **adm.fitvt.ru**, **st.fitvt.ru**, **test.fitvt.ru** – административная, учебная и тестовая подсети соответственно. Однозначное соответствие элементов физической и логической инфраструктур сети в дальнейшем изложении позволяет использовать термины «подсеть» и «поддомен» как синонимы.

2.1. Внутренняя структура каждого из поддоменов состоит из одинаковых базовых элементов. По необходимости в каждом из поддоменов будут размещены сервера со специфическими ролями.

Общие части структуры поддоменов мы рассмотрим на примере **st.fitvt.ru**. Специфические серверные роли для каждой подсети описаны позднее.

Схема поддомена **st.fitvt.ru** представлена на **рисунке 1**.

Рис. 1.

Каждый из поддоменов будет содержать один или два контроллера домена (DC) с базой данных Активного каталога (AD), один сервер разрешения имен (DNS), один DHCP-сервер, один Web-сервер, один подчиненный сервер сертификатов (SCA), один межсетевой экран (ISA), используемый для соединения подсетей друг с другом и с Интернетом. Возможно, отдельных DNS-серверов в подсетях не будет. Эту роль можно совместить с ролью контроллера домена. Это даст следующее преимущество: базу данных доменных имен можно интегрировать в активный каталог и разрешить только безопасные обновления записей ресурсов в этой базе. Таким образом, только прошедшие на контроллере домена проверку структуры (пользователи или компьютеры) смогут изменять записи доменных имен. Это безусловный плюс безопасности, который в принципе избавляет сеть от атак типа *redirect*.

DHCP-сервера обязательно должны быть размещены в студенческой и тестовой подсетях, а в административной подсети надобности в этом сервере из-за малого числа клиентских компьютеров. В учебной подсети понадобятся DHCP-ретрансляторы, т.к. все важные сервера предполагается сосредоточить в одном помещении, а не расставлять по учебным аудиториям.

На Web-серверах будут размещаться внутренние сайты факультета, виртуальные каталоги и FTP-ресурсы студентов, Web-сервера предполагается развернуть на основе технологии IIS 6.0.

Подчиненный сервер сертификатов будет использоваться для выдачи сертификатов клиентским компьютерам и для аутентификации их на контроллере домена при подключении через VPN. Это особенно актуально для студенческой подсети, т.к. именно в ней таких подключений будет большинство. Также сервер сертификатов будет использоваться для выдачи технических сертификатов серверам подсети. Их количество и описание может варьироваться в зависимости от производственной надобности и выходит за рамки данной статьи.

Брандмауэры предполагается установить во всех подсетях. Причем в студенческой подсети не предполагается наличие демилитаризованной зоны (DZ), а в остальных подсетях будут размещены два межсетевых экрана.

При большом числе VPN-подключений и Интернет-запросов один ISA-сервер скорее всего не будет справляться с работой, что вызовет неоправданные временные задержки в отображении Web-страниц и подключений к внутренним ресурсам сети. Для решения этой проблемы в студенческой подсети необходимо развернуть массив из двух-трех ISA-серверов, организованных как NLB-кластер с одним виртуальным ip-адресом.

Клиентские компьютеры во всех подсетях будут настроены как клиенты DNS, DHCP, и Web-proxy одновременно. В каждой подсети будут развернуты сервера кэширования и автоматического обновления (SUS). Эти функции можно отдать ISA-серверу, если это не вызовет его перегрузку. Аппаратных брандмауэров и маршрутизаторов устанавливать не предполагается.

В студенческой подсети необходим кластер серверов приложений, содержащий три-четыре компьютера с установленными на них лицензионными средами разработки и другими необходимыми средствами и кластер серверов баз данных. Все кластеры предполагается организовать на основе технологий NLB. В случае необходимости Web-кластер можно организовать, используя обыкновенные «зеркала» и настроив циклическую расстановку на серверах DNS.

Административная подсеть является копией учебной за исключением кластеров приложений и баз данных. Также в этой сети нет необходимости в массиве ISA-серверов и их настройке в качестве Web-proxy. Теоретически и в данной сети может возникнуть необходимость в DHCP-сервере, в случае если количество доступных на кафедрах портативных компьютеров резко возрастет.

Тестовая подсеть является копией студенческой подсети с той лишь разницей, что количество клиентских компьютеров мало, нет массива межсетевых экранов и кластера баз данных. Подчиненный сервер сертификатов тестовой подсети будет ограничен в возможностях: он будет выдавать сертификаты только для аутентификации в пределах подсети. Студенты-администраторы этой подсети не будут иметь административных полномочий на внешнем брандмауэре демилитаризованной зоны.

2.2. Предполагается разделить сеть на три части: *внутреннюю*, *внешнюю* и *сеть перим*етра. Во внутренней подсети будут находиться административный

и учебный поддомены. Во внешней - пользователи Интернета и удаленные VPN-клиенты. В сети периметра – тестовый поддомен и контроллеры доменов студенческой и административной подсетей, находящихся в соответствующих демилитаризованных зонах.

Принцип разделения сети на зоны обуславливает определенное количество сетевых интерфейсов на ISA-серверах и контроллерах доменов. В ISA-серверах их должно быть не менее трех, а на контроллерах доменов не менее двух. Это влечет определенные трудности при выборе стратегии ip-адресации, организации кластеров и обеспечению избыточности, учитывая произвол в предоставлении провайдерами внешних ip-адресов.

Для выдачи сертификатов подчиненным серверам в сети необходимо развернуть корневой сервер сертификации (RCA). Как базовый элемент системы безопасности сети он не будет входить ни в какие домены и должен быть установлен в отдельном помещении, желательно в сейфе. Доступ к нему должен быть только у старшего администратора сети. Этот сервер не должен подключаться в корпоративную сеть факультета, он должен оставаться изолированным, а выданные им сертификаты должны устанавливаться на подчиненные сервера сертификации старшим администратором сети при помощи переносных носителей.

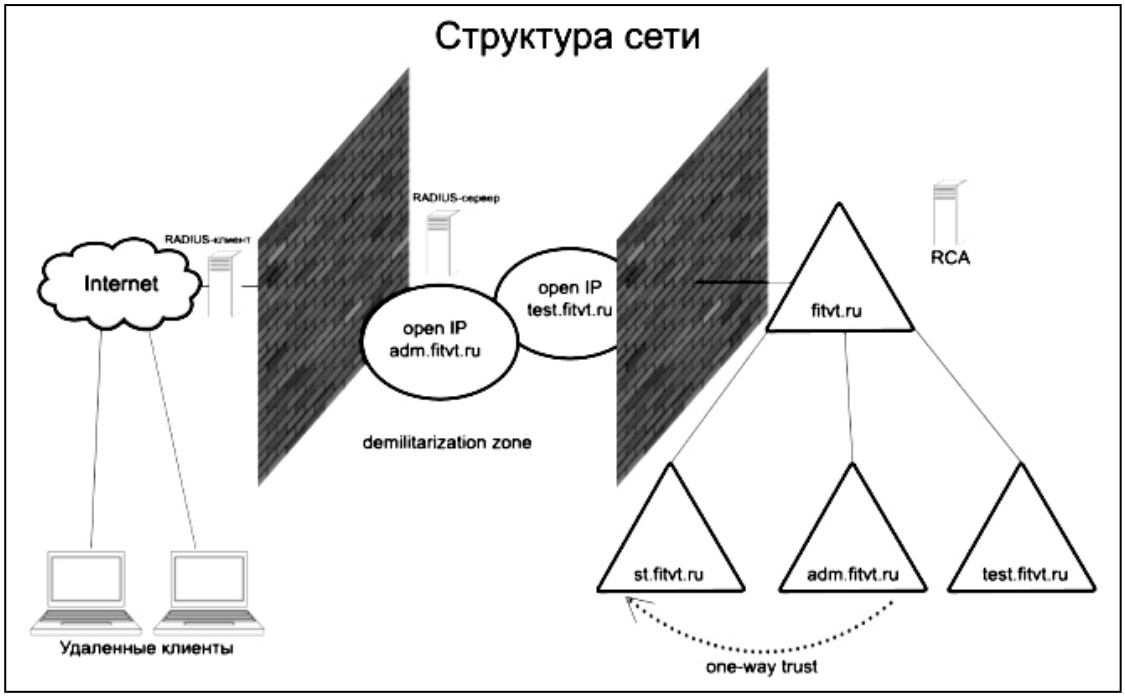

Схема сети представлена на рис. 2.

Рис. 2.

Между административным и учебным поддоменом предполагается установить одностороннее доверие. В этом случае пользователи, прошедшие проверку на контроллерах административного поддомена, будут иметь доступ к ресурсам учебного поддомена без повторного опознавания, а пользователям учебной подсети нужно аутентифицироваться повторно при доступе к ресурсам административной подсети.

Межсетевые экраны предполагается оставить настроенными по умолчанию, что означает, что все порты и все протоколы связи на первом этапе будут закрыты и запрещены. Открывать порты и устанавливать разрешающие прави-

ла для протоколов предполагается по мере необходимости, после детального анализа исходящего сетевого трафика в поддоменах.

Для обеспечения отказоустойчивости на Web-серверах предполагается установить аппаратные RAID-5 контроллеры и не менее четырех жестких дисков. Также предполагается проводить ежемесячную полную архивацию контроллеров доменов, клиентских компьютеров административного поддомена, DNS-серверов, Web-серверов и серверов баз данных. Также планируется проводить разностные архивации указанных объектов в течение недели по установленному графику. Такая стратегия архивации требует большого количества свободного дискового пространства, но позволяет восстановить систему после сбоя за наименьшее время. Носители с архивами рекомендуется хранить в надежном защищенном месте.

Обслуживать сеть должна команда администраторов. Роли каждого из них должны быть четко разделены. Во-первых, необходимо выделить группу администраторов поддоменов, у которых будут всеобъемлющие права доступа в пределах своих подсетей. Создать группу операторов архива – они будут иметь возможность архивировать и восстанавливать систему после сбоя в пределах своих поддоменов. Создать группу операторов серверов - они будут следить за производительностью серверных систем, и оценивать показания счетчиков по сравнению с «базовой линией».

В сети должен быть один или два старших администратора, имеющих права полного доступа в пределах всей сети.

Совмещать указанные должности крайне не рекомендуется.

Пользователи сети получают разрешения на доступ к объектам от администраторов своих поддоменов. По умолчанию при создании нового пользователя в активном каталоге для него создается папка профиля, выделяются места на Web-сервере согласно установленной квоте и даются разрешения на запуск необходимых программ. Остальные ресурсы сети остаются для него закрытыми. Получить к ним доступ можно только по согласованию с администратором.

Стратегия ip-адресации, правила архивирования, квалификационные требования к администраторам серверов и членам других сервисных групп, разрешающие правила брандмауэра, квотирование дискового пространства и прочие элементы безопасности должны быть утверждены в форме единого документа приказом декана и соблюдаться неукоснительно.

Карпенко О.М., Бершадская М.Д., Гадрани Л.А.

МЕГАУНИВЕРСИТЕТЫ КАК ОПТИМАЛЬНЫЙ ПУТЬ РАЗВИТИЯ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

plan@muh.ru
НОУ Современная гуманитарная академия
г. Москва

Новым этапом в развитии высшего образования на рубеже веков стало появление и стремительный рост мегауниверситетов - особой категории высших учебных заведений, которые, по выражению Джона Дэниэла, «являются